

أشهر الخرافات
في مجال الحماية والامان

تاليف:
ابراهيم العايدي

المحتوى

مقدمة

لعل أول واهم المصطلحات التي جرت في مخيلتنا حينما قمنا باستخدام لكمبيوتر لأول مرة كانت هي : الحماية – الفيروسات – الاختراق و الهاكرز .. الخ . الكثير منا تابع هذه الاخبار عبر وسائل الاعلام بشغف: فهذا الفيروس تسبب في اصابة عشرات الالاف من الكمبيوترات حول العالم . نبأ عن اختراق شبكة او المواقع التابعة لشركة او جهة جهات حكومية . الخبراء يحذرون من انتشار فيروس جديد ... الخ ..

ولا شك ايضا ان الامن والحماية يحتل الاهمية و المكانة الاولى عند اي شخص يتعامل مع هذا العالم الفريد . ولكن للأسف تسببت قلة المعلومات المتوفرة والاشاعات و الافتاءات التي تصدر من اشخاص غير مختصين الي فتح الباب الي الكثير من الخرافات في مجال الحماية تحول بعضها الي "خزعبلات" صدقها الكثيرون وتسببت في الكثير من الازعاج والقلق للعديد من المستخدمين وتسبب ايضا في توليد جواهس وفوبيا من استخدام الكمبيوتر والانترنت !

لذلك قمت برصد أهم واكبر ١٠ خرافات منتشرة عند الكثير من المستخدمين .

١. هذا الانتي فيروس قاهر لكل انواع الفيروسات ويعد الأقوى في العالم !

للأسف الكثير من المستخدمين يبالغون في تقدير قوة انتي فيروس ما شهير ويضعون فيه كامل ثقتهم . سواء من خلال تجربتهم او من خلال ما قراؤه عنه . بالإضافة الي العبارات الرنانة التي قد نشاهدها علي المنتديات او المواقع التي تبالغ جدا في وصفه وبيان قوته وصلت الي حد وصفه بانه (خارق لا يسمح بمرور بعوضة !!) . من الحقائق المعروفة هو ان جميع انواع الانتي فيروسات الشهيرة في العالم لديها قدرة كبيرة علي كشف الفيروسات القديمة وبخاصة برامج التجسس Spyware بنسبة وصلت الي ٩٩% .. بينما تقل هذه النسبة كثير الي الديدان worms والفيروسات الأخرى لم تزيد عن ٩٠%.

ولكن المشكلة الاكبر التي لا يدركها البعض هي الفيروسات الجديدة . وفقا لأحدث الدراسات في مجال الحماية اثبتت ان قدرة اشهر برامج المكافحة لاكتشاف الفيروسات الجديدة لم تتخطى ٥% وهذا بالطبع امر مقلق بشدة.

ذلك لان اغلب انواع الانتي فيروس يعتمد في اسلوب الحماية علي نظامين: **البصمة الرقمية Signature** (قاعدة بيانات تحتوي علي جميع الفيروسات القديمة والحديثة واي فيروسات يتم اكتشافها، ولكل فيروس بصمة خاصة يتم كشفه من خلالها) و **اسلوب مراقبة النشاطات المريبة Heuristic** (حيث يتم مراقبة نشاط ورصد اي انشطة مريبة لأي ملف بالكمبيوتر) . ولذلك يضع اغلب صانعي الفيروسات كافة مجهودهم لتفادي الطريقة الثانية وحيث ان الفيروس جديد فلا يوجد له بصمة الكترونية علي اي قاعدة بيانات لأي انتي فيروس . مما يجعل مهمة الفيروس سهلة خلال هذه الفترة حتي ينكشف امره ويتم رصده . لذا فان فكرة الاعتماد الكلي علي اسم شهير لأي انتي فيروس فقط هو خطا جسيم للأسف لا يدرك ذلك الكثيرون .

٢. برنامج يمكنه استرجاع او سرقة باسورد اي ايميل !

واحدة من اشهر الخرافات التي انتشرت بشدة علي المواقع العربية ولا تزال. وهو ايمان البعض بوجود برنامج او طريقة ما لجلب باسورد ايميل معين . ولكن بالطبع هذا الامر في حد ذاته غير منطقي بالمرة !

اي باسورد لأي ايميل او حساب ما لا يعرفه سوي اثنين : قاعدة البيانات لهذا الموقع - صاحب الحساب /الايميل

بالتأكيد صاحب الحساب غير معروف مكانه. وحتي لو عرف ذلك البرنامج لن يطرق بابه ويقول له اعطني باسورد ايميلك من فضلك ! (: .. اذن لا يتبقى سوي قاعدة بيانات او سيرفرات المواقع .. بالتأكيد حينما نتحدث عن شركات الشهيرة مثل: الياهو وجوجل و فيسبوك وهوت ميل وغيرها هي ليست بموقع دردشة او منتدي يستطيع اي شخص دخولها او اختراقها . لان هذه الشركات تنفق علي حمايتها ميزانيات تعادل ميزانيات دول صغيرة ! بل تكاد تكون اكبر من ميزانية حماية الحكومة الامريكية نفسها ! ذلك لان صلب وجوهر الشركة وسمعتها تعمد علي حماية بياناتها وبيانات مشتركيها . وحينما يكون قيمة هذه الشركات بعشرات المليارات من الدولارات فتخيل المبالغ التي قد ترصد لذلك !

لذلك لا تتخيل ابدا ان مجرد برنامج صغير علي منتدى او وجود طريقة ما خارقة قادرة علي ذلك بسهولة . والا اصبح بمقدور اي شخص سرقة ما يحلو له من الايميلات ولن يصبح لها فائدة بعد ذلك !

الشيء اللي لاحظته في هذه النوعية من البرامج او المواقع انها خداعية تقوم بسرقة ايميلك انت شخصيا وليس الضحية . لاني لاحظت انه يطلب منك بسذاجة ان تقوم بإدخال اسمك وباسوردك و يدعي انه يقوم بعملية ما وهي ليست الا مجرد حيلة تتسبب في سرقتك انت . وللعلم هذه البرامج ايضا تتخذ اشكال اخري توهمك انها قادرة علي اختراق المواقع مثل : اضافة ذهب او رصيد لألعاب الفيس بوك وغيرها !!

٣. الهاكرز لديهم طرق سحرية خاصة لاختراق اي موقع او اي جهاز في العالم !

لا شك ان مجال الاختراق او الهاكرز يحوز علي اهتمام وشغف الكثيرون منا . والاخبار التي تتعلق بذلك المجال تثير دهشة واعجاب البعض منا وخاصة الاعجاب بهؤلاء المخترقين الذي يصل حد الاعجاب بهم الي درجات المبالغة وتصديق خرافات لا صحة لها . يعتقد الكثير من المستخدمين ان هؤلاء المخترقين او الهاكرز اشخاص غير طبيعيين اشبه بالسحرة لديهم طرق خاصة قادرة علي اختراق اي جهاز او موقع بالعالم كما يحلو لهم . او كما نشاهد بالأفلام نجد البطل قادر علي اختراق اي سيرفرات للاستخبارات او البنوك ببضع نقرات علي الكيبورد .. او يقوم باختراق نظام امني معين من خلال هاتف نوكيا ٩٠٠٠ (:

ولكن الحقيقة ان هذا الامر ليس حقيقي وليس بالشكل الذي يعتقده البعض . اختراق المواقع او الاجهزة ليس سهلا وليس له طرق ثابتة معينة بل تتركز المسألة علي ايجاد ثغرة يستطيع ان ينفذ منها ويسيطر عليه . لذا فان عملية ايجاد هذه الثغرة هيا ليست بالأمر السهل بل صعب جدا يصل الي الشبة مستحيل ويحتاج الي فريق ومحاولات كثيرة جدا .

لذا فان نجاح البعض في الاختراق وبعدها يضع صفحة سوداء له وجمجمة ويطلق علي نفسه اسم صقر العروبة او عقرب الصحراء او القرصان الاحمر ليس معناه انه قادر علي اختراق اي شيء اخر . ذلك لأنه ربما استطاع ذلك نتيجة انه موقع بلا حماية او ضعيف جدا وهذا الامر بالطبع ليس مع كل اجهزة الكمبيوتر او المواقع .

٤. نظامي التشغيل لينكس او ماك لا يحتويان علي فيروسات او لا يمكن اختراقهما !

لعل هذا الامر شائعة جدا عند مستخدمي نظامي التشغيل لينكس وماك. نتذكر جميعا اعلان ابل الشهيرة I'm mac حينما كان يسخر من ويندوز ومن احد الاسباب وجود فيروسات عليه بينما الماك لا . ولعل ايضا مستخدمي لينكس وتوزيعاتها المختلفة يروجون لهذا الامر بشدة عند الحديث عن مميزات لينكس . والكثيرون ايضا يروجون ان نظام ويندوز هو فقط من يحتوي علي فيروسات ويسهل اختراقه. بنما الانظمة الأخرى نظيفة لا تحتوي علي فيروسات. كل هذه المعتقدات السابقة ثبت انها غير صحيحة بالمرة .

فهذه الانظمة تعرضت للكثير من الفيروسات الخطيرة طيلة السنوات الماضية ولعل اشهرها فيروس Leap-A و Hong Kong و HellRTS و Flashback لنظام تشغيل ماك . وايضا فيروس Diesel و Lion و الدودة Devnul . بالإضافة الي العديد من الهجمات والاختراقات التي اصابت كلا النظامين في السنوات الاخيرة .

ولكن المسألة قد تبدو نسبية في هذا الامر . فالحقيقة ان نظام ويندوز نسبته كبيرة جدا في الاصابة بفيروسات واختراقات مقارنة بماك ولينكس ذوي نسبة اصابة قليلة . ولكن هذا الامر يرجع الي النسبة الضخمة جدا لاستخدام ويندوز عالميا (٩٠% تقريبا) مما يجعل بالتأكيد صانعي الفيروسات يوجهون اغلب نشاطهم اليها اكثر من الاخرين . ايضا شهرته الواسعة جعلت اغلب ثغراته معروفة (خاصة ويندوز XP) اكثر من باقي الانظمة الأخرى . كما اكدت بعض الدراسات ان نظامي لينكس وماك لا يتمتعان بحماية اكبر من الويندوز في التعرض للفيروسات او الاختراقات . بل يوجد بهما ثغرات خطيرة يسهل اختراقها ونشر فيروسات بهما .

لذا فان اعتقادك ان نظامي ماك او لينكس خاليين من الفيروسات او ل يمكن اختراقهما هو امر عاري تماما من الصحة .

٥. الفيروس يمكنه ان يتسبب في انفجار الكمبيوتر او اتلافه اجزاءه !

خرافة اخري صدقها البعض نتيجة الاشاعات او حسبما كنا نشاهد في الافلام الامريكية . فنجد الفيروس يجعل الكمبيوتر ينفجر او يحترق او يتم تدمير جزء من الاجزاء الصلبة Hardware كل هذه الامور غير حقيقية ولا يمكنها ان تتحقق. الفيروس ما هو الا برمجة تأثيرها يكون مقصورا علي النواحي البرمجية، او لديه قدرة علي اصدار اوامر في نظام التشغيل قد تسبب ضررا مثل : مسح البيانات من علي القرص – مسح التعريفات .. الخ

ولم نسمع عن فيروس قام بتدمير كارت الشاشة مثلا او الرام او البروسيسور او اتلاف القرص الصلب تماما . حتي فيروس تشيرنوبيل الشهير والمعروف اختصارا بـ CIH كانت قدرته هي تخريب البيوس BIOS او مسح سجل البوت الرئيسي Master Boot او partition table للقرص الصلب مما يجعله غير قابل للقراءة . ولكن تم ايجاد طرق لعلاج هذه التأثيرات . بنما كانت الاجزاء الصلبة تم يمسحها الضرر .

٦. عند فتح الايميل لا يمكن ان يصاب جهازك بالفيروس.

حتي كتابة هذه السطور كنت مقتنع بهذه الامر . فالاعتقاد السائد هو عندما تتصفح رسالة قد تحتوي علي فيروس لن تصاب بضرر اذا قمت بتصفح الرسالة فقط . ببنما تصاب بالضرر عندما تقوم بفتح الملف المرفق مع الرسالة او الضغط علي رابط ما . ولكن لكون عملي مطور ويب اثار هذا الامر شكوكي حتي تأكدت منه تماما . فمن المعروف ان الايميلات تكون مكتوبة بلغة HTML ولذلك يمكن بسهولة ادراج اكواد جافا سكربت او ضع الفيروس داخل الصورة او Iframe مما قد يسمح يتحميل ملف الفيروس الي جهازك دون ان تشعر . ولكن هذه المسألة ربما تكون صعبة هذه الايام لوجود انظمة متطورة لفحص للايميلات او تعطيل اكواد معينة ولكن هذا لا يمنع من قيام مبرمج محترف من عمل ذلك دون ان ترصدها انظمة الحماية . لذلك اعتقادك بان تصفح الايميل امن ولن تصاب بفيروس هو امر خاطئ تماما .

٧. طالما الجهاز سليم ويعمل بشكل طبيعي . لا يوجد فيروسات !

احد الاعتقادات الخاطئة عند الكثير من المستخدمين . طالما نظام التشغيل يعمل بكفاءة ولم يلاحظ اي امور مريبة فهذا يعني ان الجهاز خالي من الفيروسات . بالتأكيد اعتقاد خاطئ .
حيث يمكن ان يكون جهازك به فيروس ولم يتم كشفه بعد (راجع الفقرة ١) . او يكون الفيروس قوي بشكل يمكنه تجنب برامج الحماية . او يكون الفيروس لديه توقيت معين للتنشيط (مثل فيروس تشيرنوبيل) او قد يكون مخصص لأداء هدف اخر غير معلن مثل ان يكون برنامج تجسسيا او لسرقة البيانات . اغلب الفيروسات تتخذ طابع تمويه وليست كما يظهر بالأفلام يظهر علي الشاشة رسالة مرعبة او جمجمة تضحك او غيرها من هذه الامر . لذا لا تنخدع بهذا الامر !

٨. تعطل الكمبيوتر سببه وجود فيروسات به .

الاعتقاد الشائع عن نسبة كبيرة جدا من المستخدمين . بل قد يكون السبب الاول الذي يقفز في رأسك عندما يتعطل الويندوز او تظهر رسائل الخطأ كثيرا. ليس بالضرورة عند حدوث ذلك ان يكون بسبب فيروس ما في جهازك . فقد يكون هذا نتيجة عطل في نظام التشغيل او القرص الصلب او الرام او اي امر اخر . هناك اسباب اخري قد تؤدي الي ذلك .

٩. هذا الاسم او الايميل مملوك لهاكر لا تضيفه عندك حتي لا يسرق ايميلك

احد الخرافات الساذجة السخيفة التي انتشرت بشدة عبر المنتديات والمواقع الاجتماعية والجروبات والايميلات . فهو امر غير صحيح تماما للأسباب التي وضحناها في الفقرة الثانية . فلا يعقل ان اضافة شخص ما لديك قد يسبب في سرقة ايميلك !

ولكن الحقيقة في هذا الامر هو ان هذا الشخص المذكور حينما يتحدث معك قد يرسل لك صورة او ملف او يقول لك افتح الموقع كذا . مما يؤدي الي تحمل تروجان Trojan او برنامج لاقط للوجه المفاتيح Keylogger علي جهازك مما قد يسمح له بمعرفة كلمة السر وسرقتها .

١٠. عند الاصابة بفيروس ما . قم بعمل فحص شامل .

الخطأ الشائع الذي يقوم به اغلب المستخدمين عند اصابتهم بفيروس ما . يقومون فورا بعمل فحص Scan شامل للجهاز كله معتقدين ان ذلك سيخلصهم من الفيروس المزعج . هذا الامر ليس خاطئ بنسبة ١٠٠% بل احيانا يكون مفيد ويستطيع اكتشاف وازالة هذا الفيروس المزعج وهذه الطريقة ايضا تكون مجدية مع الفيروسات الشائعة. ولكن هذا الامر ليس كافيا ولا يحدث مع جميع الفيروسات فالفيروسات لها طابع خداعي كما ذكرنا من قبل واحيانا الفحص يقوم بإزالة اجزاء منه .

من الاخطاء الشائعة ايضا في هذا الامر قيام المستخدم بإعادة تنصيب نظام التشغيل . هذا ايضا غير كافي ولا يقضي تماما علي الفيروس لأنه قد ينسخ نفسه في البارتشنات الأخرى مما يسمح بعودته مرة اخري !

***



- http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html
- http://www.channelregister.co.uk/2007/12/21/dwindling_antivirus_protection/
- https://en.wikipedia.org/wiki/Antivirus_software
- http://mac-antivirus-software-review.toptenreviews.com/history-of-macintosh-viruses.html
- http://askleo.com/can_i_really_catch_an_email_virus_just_by_looking/